



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/648,149

08/25/2003

William H. Saito

IOSOFTW.003A

3524

20995

7590

12/04/2006

KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614

EXAMINER

LANIER, BENJAMIN E

ART UNIT

PAPER NUMBER

2132

DATE MAILED: 12/04/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/648,149	SAITO, WILLIAM H.	
	Examiner	Art Unit	
	Benjamin E. Lanier	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-30 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-30 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

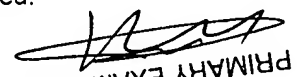
Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 25 August 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.


KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____. |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date ____. | 6) <input type="checkbox"/> Other: ____. |

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-5, 7-10, 13-18, 20-22, 25-27, 29, 30 are rejected under 35 U.S.C. 102(b) as being anticipated by Nobrega, U.S. Publication No. 2002/0107791. Referring to claims 1, 13, Nobrega discloses a method and apparatus for performing a credit transaction using a wireless communication device wherein an entity such as a wireless carrier maintains, owns and/or operates a commerce platform within a trusted domain ([0022]), which meets the limitation of a controller. The commerce platform stores the consumer's credit card account information and other personal information on the consumer ([0022]), which meets the limitation of at least one record that includes information about each of the plurality of individuals. The merchant's point of sale (POS) terminal sends transaction information to the acquirer at the time of purchase ([0022]), which meets the limitation of at least one secure component. The identities of the credit card users are validated using the cellular telephones of the user performing the transaction ([0020]), which meets the limitation of individuals having communication devices. A unique ID, which can be the user's cell phone number ([0065]), is used by the commerce platform to identify the user account ([0065]-[0066]), which meets the limitation of the information about the plurality of individuals including a communication path which defines how to contact the individual's communication device. Verification of the user is performed by comparing a stored

PIN against a user entered PIN ([0066]), which meets the limitation of the information about the plurality of individuals including a security protocol for allowing access to the secure component. The consumer communicates the unique ID to the merchant directly from the wireless device to the merchant's equipment ([0065]), which meets the limitation of input of the at least one secure component in response to the individual manipulating the input device. This unique ID is then transmitted to the commerce platform ([0065]), which meets the limitation of the controller receives the signals from the input of the at least one secure component in response to the individual manipulating the input device. The commerce platform maps the unique ID to the appropriate wireless carrier ([0065]), verifies that the cell phone involved in the transaction is in the same geographic area as the merchant ([0066]), sends transaction details to the consumer phone ([0066]), and prompts the consumer to enter their PIN into the cell phone ([0066]), which meets the limitation of the controller, in response to one of the individuals seeking access to the at least one secure component, retrieves the security protocol and the communication path from the at least one record, a communication interface allows signals between the communications device carried by the individual and the controller wherein the controller (i) evaluates the signal received from the input device of the secure component, (ii) sends a first signal to the communications device of the individual in response to the individual seeking access to the at least one secure component. The consumer transmits the entered PIN to the commerce platform where it is used to verify the user's identity against previously established accounts ([0066]), which meets the limitation of a controller having access to the at least one record, and (iii) evaluating a response signal by the individual by comparing the response signal to the security

protocol to determine whether to allow access by the individual to the at least one secure component.

Referring to claim 2, Nobrega discloses that the commerce platform prompts the consumer to enter their PIN into the cell phone ([0066]). The consumer transmits the entered PIN to the commerce platform where it is used to verify the user's identity against previously established accounts ([0066]), which meets the limitation of the security protocol comprises sending a prompt signal to the individual via the communications interface prompting the individual to enter and transmit an access code using the communications device and then comparing the access code to a pre-recorded code stored in the at least one record to ascertain whether the individual correctly entered and transmitted the access code.

Referring to claims 3, 4, Nobrega discloses that the commerce platform verifies that the cell phone involved in the transaction is in the same geographic area as the merchant ([0066]), which meets the limitation of the at least one record further includes additional security criteria and wherein the controller allows access to the at least one secure component only when the individual has satisfied the security protocol and the additional security criteria, the additional security criteria includes location information from which the individual must send the access code and wherein the individual's communication device transmits location information when transmitting the access code to the communications interface such that the controller can evaluate the additional security criteria.

Referring to claim 5, Nobrega discloses that the consumer communicates the unique ID directly from the wireless device to the merchant's equipment ([0065]), which meets the limitation of the security protocol comprises sending an access code to the user via the

communications interface and then evaluating whether the individual correctly entered the access code on the input of the at least one secure component because the unique ID can be a cell phone number ([0065]) or credit card number alternative ([0066]) that is used by the commerce platform to identify the user account ([0066]), and because the commerce platform is maintained and operated by a wireless carrier ([0040]), the cell phone number would be transmitted from the wireless carrier to the cell phone.

Referring to claim 7, Nobrega discloses that the consumer cell phone and the commerce platform are connected using a wireless network (Figure 2, element 21 & [0043]), which meets the limitation of the communications interface comprises a modem that is adapted to provide cellular telephone communication between the controller and cellular telephone devices carried by the plurality of individuals.

Referring to claims 8, 20, Nobrega discloses that the commerce platform may be maintained and operated by a wireless carrier which provides telecommunications services to the wireless device involved in the credit card transaction ([0040]), which meets the limitation of the at least one record further includes supplemental commands and corresponding actions wherein the controller, in response to receiving a supplemental command from a user, induces the system to implement the corresponding action because the wireless carrier provides supplemental services to the wireless device in the form of credit card transactions where cellular telecommunications services are the normal services provided.

Referring to claims 9, 10, 21, 22, Nobrega discloses commerce platform provides for the cell phone an Internet portal that provides access to an e-commerce software application ([0046]), which meets the limitation of the supplemental command comprises an additional

access code provided to the controller via the communications interface by the individual communications device that induces the controller to limit access to the at least one secure component because the cell phone would have to identify, using a URL, the particular e-commerce facility to access.

Referring to claim 14, Nobrega discloses that the wireless communication device may be a cellular telephone or PDA ([0033]), which meets the limitation of the communication interface comprises a telephone modem that transmits signals to cellular telephones or cellular telephone enabled PDAs that comprise the communication devices of the individuals.

Referring to claim 15, Nobrega discloses that the consumer transmits the entered PIN to the commerce platform where it is used to verify the user's identity against previously established accounts ([0066]), which meets the limitation of the access code is received by the controller via the individual's communication device via the communications interface.

Referring to claim 16, Nobrega discloses that the consumer communicates the unique ID to the merchant directly from the wireless device to the merchant's equipment ([0065]). This unique ID is then transmitted to the commerce platform ([0065]), which meets the limitation of the controller interfaces with the one or more secure components and wherein the one or more secure components includes an input such that signals entered on the input are received by the controller.

Referring to claim 17, Nobrega discloses that the commerce platform (Figure 2, element 2) is networked (Figure 2, element 26) to the merchant POS (Figure 2, element 5), which meets the limitation of the controller is networked with the one or more secure components.

Referring to claim 18, Nobrega discloses that the commerce platform prompts the consumer to enter their PIN into the cell phone ([0066]). The consumer transmits the entered PIN to the commerce platform where it is used to verify the user's identity against previously established accounts ([0066]), which meets the limitation of the access code is received by the controller via the input device of the secure component following the controller transmitting a prompt signal to the individual's communication device.

Referring to claim 25, Nobrega discloses a method and apparatus for performing a credit transaction using a wireless communication device wherein an entity such as a wireless carrier maintains, owns and/or operates a commerce platform within a trusted domain ([0022]), which meets the limitation of a controller. The commerce platform stores the consumer's credit card account information and other personal information on the consumer ([0022]). The merchant's point of sale (POS) terminal sends transaction information to the acquirer at the time of purchase ([0022]). The identities of the credit card users are validated using the cellular telephones of the user performing the transaction ([0020]). A unique ID, which can be the user's cell phone number ([0065]), is used by the commerce platform to identify the user account ([0065]-[0066]). Verification of the user is performed by comparing a stored PIN against a user entered PIN ([0066]). The consumer communicates the unique ID to the merchant directly from the wireless device to the merchant's equipment ([0065]), which meets the limitation of receiving a signal from an input of the secure component indicative of the individual seeking access to the secure component. This unique ID is then transmitted to the commerce platform ([0065]). The commerce platform maps the unique ID to the appropriate wireless carrier ([0065]), verifies that the cell phone involved in the transaction is in the same geographic area as the merchant

Art Unit: 2132

[[0066]], sends transaction details to the consumer phone ([0066]), and prompts the consumer to enter their PIN into the cell phone ([0066]). The consumer transmits the entered PIN to the commerce platform where it is used to verify the user's identity against previously established accounts ([0066]), which meets the limitation of receiving an access code from an individual seeking access to the secure component, comparing the access code to a stored access code, communicating with the individual's portable communication device, allowing access to the secure component when the access code received from the individual matches the stored access code component when the access code received from the individual matches the stored access code and when the individual has communicated with the system via their portable communication device.

Referring to claim 26, Nobrega discloses that the commerce platform may be maintained and operated by a wireless carrier which provides telecommunications services to the wireless device involved in the credit card transaction ([0040]), which meets the limitation of communicating with the individual's portable communication device comprises sending cellular telephony signals to the individual's cellular telephone enabled device.

Referring to claim 27, Nobrega discloses that the consumer transmits the entered PIN to the commerce platform where it is used to verify the user's identity against previously established accounts ([0066]), which meets the limitation receiving the access code comprises receiving the access code from the individual's portable communication device.

Referring to claim 29, Nobrega discloses that the commerce platform may be maintained and operated by a wireless carrier which provides telecommunications services to the wireless device involved in the credit card transaction ([0040]), which meets the limitation of the at least

Art Unit: 2132

one record further includes supplemental commands and corresponding actions wherein the controller, in response to receiving a supplemental command from a user, induces the system to implement the corresponding action because the wireless carrier provides supplemental services to the wireless device in the form of credit card transactions where cellular telecommunications services are the normal services provided.

Referring to claim 30, Nobrega discloses that if verification fails, an appropriate message is sent to the phone, and the transaction is terminated ([0066]), which meets the limitation of implementing the action corresponding to the supplemental command comprises disabling portions of the secure component from access.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

5. Claims 6, 19, 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nobrega, U.S. Publication No. 2002/0107791. Referring to claims 6, 19, 28, Nobrega discloses that the

commerce platform prompts the consumer to enter their PIN into the cell phone ([0066]), which meets the limitation of sending a prompt signal to the individual via the communications interface prompting the individual to enter and transmit a first access code using the communications device. The consumer transmits the entered PIN to the commerce platform where it is used to verify the user's identity against previously established accounts ([0066]), which meets the limitation of comparing the first access code to a pre-recorded access code stored in the at least one record to ascertain whether the individual correctly entered and transmitted the first access code. The commerce platform then causes the consumer's phone to prompt the consumer to indicate the method of payment ([0066]). The consumer selects the method of payment and transmits the selection to the commerce platform ([0066]), which meets the limitation of sending a second access code to the communications device in response to determining that the individual correctly entered and transmitted the first access code. Once the transaction is approved a digital receipt containing the approval authorization number is made available to the cell phone ([0051]), which meets the limitation of sending a second access code to the communications device in response to determining that the individual correctly entered and transmitted the first access code. The approval authorization number is also transmitted to the merchant POS terminal. Nobrega does not disclose that the consumer enters the approval authorization number into the merchant POS terminal. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have the consumer enter the approval authorization number obtained from the digital receipt into the merchant POS so that the merchant POS could verify that the consumer approved the correct transaction since no physical signature is utilized as taught by Nobrega ([0052]).

Art Unit: 2132

6. Claims 11, 12, 23, 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nobrega, U.S. Publication No. 2002/0107791, in view of Fung, U.S. Patent No. 6,859,882. Referring to claims 11, 12, 23, 24, Nobrega discloses commerce platform provides for the cell phone an Internet portal that provides access to an e-commerce software application ([0046]). Nobrega does not disclose that the commerce platform remotely enables the e-commerce site when the cell phone consumer requests access. Fung discloses an e-commerce system where sites are remotely enabled using wake on lan signal events (Col. 69, line 53 – Col. 70, line 4), which meets the limitation of the controller is adapted to remotely enable the secure component when the controller receives an enablement signal from the individual via the communications interface, the controller remotely enables the secure component by sending a wake on lan signal to the at least one secure component. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the e-commerce sites of Nobrega to be remotely enabled by the commerce platform using wake on lan signal events in order to conserve power based on the varying demand that may be placed on the e-commerce site as taught in Fung (Col. 34, lines 7-39)

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Alonso, U.S. Patent No. 6,434,700

Lun Yip, U.S. Publication No. 2002/0147913

Johnson, U.S. Patent No. 6,535,726

Johnson, U.S. Patent No. 7,039,389

Art Unit: 2132

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805.


The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Benjamin E. Lanier


KAMBIZ ZAND
PRIMARY EXAMINER